DIGITALEUROPE

DIGITALEUROPE position on draft Indian Data Protection Bill 2018

Brussels, 18 September 2018

INTRODUCTION

DIGITALEUROPE welcomes the opportunity to submit comments on the draft Indian Personal Data Protection Bill 2018. As the voice of the technology industry in Europe, our association has been deeply involved in the negotiations that led to the adoption of the General Data Protection Regulation (GDPR), which shares similar concepts and approaches with the current Indian draft legislation.

The GDPR negotiations have strived to achieve a complex balance in ensuring strong protection while still enabling innovation and data flows, both within Europe and with foreign jurisdictions. We hope our experience in the drafting of the GDPR – and now its implementation – can help in advising on a Data Protection Bill 2018 that reflects a workable outcome.

Of particular concern to us are provisions aiming to impose data localisation. While the GDPR provides for very detailed instruments for transfers outside the European Economic Area, the objective of the European framework is still that of *enabling* cross-border data flows, subject to appropriate safeguards, rather than imposing local storage. The different goals of the Bill would not only hurt the Indian economy but ultimately also undermine the privacy and security of Indians' personal data.

Finally, we note that several key concepts in the draft bill are left to be determined through codes of practice, by the Government or the Data Protection Authority (DPA) well after enactment. This makes the full impact of the proposed law difficult to predict in its entirety, leaving companies unable to shape in detail their compliance programmes as well as their internal practices and processes. DIGITALEUROPE urges that companies should have the necessary time to understand and implement the rules after all these determinations take place. Companies operating in Europe have found that the two-year implementation period foreseen by the GDPR, which was set to allow companies to take all necessary steps, was absolutely essential.

PRIORITY RECOMMENDATIONS

1. **Data localisation requirements do not improve data protection** and severely disrupt operations and security capabilities of both fiduciaries and processors. More useful is a recognition of existing international data protection mechanisms – such as EU standard contractual clauses and BCRs or the Asian Pacific Economic Cooperation (APEC) forum's Cross Border Privacy Rules (CBPRs) – or a general obligation on fiduciaries and processors to be accountable and act as responsible data stewards wherever the data is processed (based on the Canadian example).
2. **The definition of personal data should be pragmatic and risk-based.** It should not include all data that is capable of reidentification by a person or set of persons but data for which a fiduciary or processor is *reasonably likely* to have and use the means to be able to identify the principal.

3. **Sensitive personal data should be reserved for categories of data that carry special risks in relation to discrimination and abuse of fundamental rights.** Passwords, official identifiers and financial data are all regularly processed by fiduciaries and processors and, while important, should not qualify for this special category. Given the broad definition of sensitive data, the limited available grounds for processing are troubling. We recommend narrowing the definition of sensitive data and introducing reasonable and employment purposes as grounds for processing sensitive data.

4. Whilst we understand the desire for the DPA to be able to conduct investigations in the form of data audits, **there should not be a general obligation for fiduciaries to undertake annual audits conducted by registered auditors**. This is neither targeted nor does it reflect that data protection programmes are often managed globally.

5. **Breaches should be notified to the DPA only if there is a real risk of significant material harm to principals. It would be preferable not to set an explicit deadline for notification but to require notification 'without undue delay.'** The timeline for notification should only begin when the responsible team within the fiduciary is aware of the breach and has a sense of its general significance – not when the breach occurs. Fiduciaries should have the right to voluntarily notify data principals prior, or in parallel, to notification of the DPA.

6. Criminal offences, as opposed to civil liabilities, are better described under more specific areas of the penal code – not in the Act. Moreover, **to the extent that natural persons are acting in the official capacity of the legal person that employs them, they should not be held personally liable**.

DETAILED ANALYSIS

1. Cross-border transfer (sections 40-41)

- Data localisation requirements, including the general obligation to store a copy of data in India and to only process critical data in India, do not improve data protection. As explained in the Report (p. 82), the objective of introducing data localisation requirements should be dual: to ensure effective enforcement and to secure the critical interests of the nation. We do not understand why it is deemed necessary and proportionate that all types of personal data processed by all data fiduciaries should at all times be stored in India – with all the costs, data governance and other complications explained below that this entails – in order to ensure that Indian data protection law applies to the data and in order to secure the critical interests of the nation. Furthermore, as mentioned in the Report, with respect to data localisation the White Paper recognised 'the need for treating different types of personal data differently and a one-size-fits-all model was not considered appropriate.' Despite this recognition, Section 40(1) of the Bill adopts a one-size-fits-all approach whereby all types of personal data must be stored in India. Such a requirement could only be justified for types of data or potentially purposes of processing that relate to the 'critical interests of the nation.'

- Data localisation requirements severely disrupt operations and the security capabilities of both fiduciaries and processors. In many cases, it is not possible to process all data locally with the same quality of service as could otherwise be achieved, such as follow-the-sun customer service. Moreover, the trend towards micro-services in service architecture and increasing distribution of data processing means that introducing such restrictions is likely to result in companies choosing not to serve the Indian market or significantly reducing functionality of their service.

- To the extent that India aims to establish data transfer mechanisms, there is scope to leverage existing international mechanisms such as EU standard contractual clauses and BCRs or the Asian Pacific Economic Cooperation (APEC) forum's Cross Border Privacy Rules (CBPRs) rather than create local versions of such mechanisms.

- Another option, following the Canadian example, that we urge India to consider is a general obligation on fiduciaries and processors to be accountable and act as responsible data stewards wherever the data is processed. Such data protection can also be guaranteed through private contractual arrangements.

2. Definitions (section 3)

- DIGITALEUROPE supports the general approach and distinctions between fiduciaries, processors and principals, which reflects the same structure found in the GDPR.

- In line with the GDPR's Recital 26, the definition of personal data should be pragmatic and risk-based. It should not include all data that is capable of reidentification by a person or set of persons but data for which a fiduciary or processor is reasonably likely to have and use the means to be able to identify the principal.

- Sensitive personal data should be reserved for categories of data that carry special risks in relation to discrimination and abuse of fundamental rights. We therefore recommend a closer alignment with the definitions laid down in the GDPR, including the definition of biometric data. Passwords, official identifiers and financial data are all regularly processed by fiduciaries and processors and, while important, should not qualify for this special category. No other jurisdiction, including the EU, has created sensitive status for these categories.

- Given the important role of the notion of 'profiling' in establishing the extra-territorial effect of the Bill (Section 2, 2(b)), similarly to the GDPR, the definition of profiling in Section 3(33) should be more granular. Profiling may be considered as a higher risk processing that merits stricter rules because it: a) takes place through automated means; and b) uses personal data in order to analyse or predict personal aspects of the individual. The current definition in the Bill encompasses all processing of personal data that analyses or predicts aspects of the individual. The definition should be amended as follows:

> 'Profiling' means any form of *automated* processing of personal data *consisting of the use of personal data to* analyse or predict *personal* aspects concerning the behaviour, attributes or interest of a data principal.

3. Principles (sections 4-11)

- There is no data protection value in requiring fiduciaries to provide notice on entities with whom data may be shared as the vendor ecosystem – not just processors but also sub-processors – is fluid and changeable over time. More relevant to the principal is understanding the types of entities with whom their data may be shared; hence, the requirement should be to notify *categories* of such entities. We would also emphasise the importance that such entities are bound to act at the direction of the fiduciary.

4. Legal grounds for processing (sections 12-17)

- DIGITALEUROPE supports the range of different grounds for processing.
- The employment purposes basis is very useful and recognises the distinct application of privacy and data protection in this sphere.
- Necessity for performance of contract should be added to the list of grounds for processing (in line with GDPR). In practice, this is one of the most important grounds for processing in everyday business. Such recognition in the Bill would be consistent with the GDPR and other frameworks.
- The draft bill departs from the GDPR's approach to 'legitimate interest' in that it leaves the determination of what types of processing can be considered 'reasonable purposes' to the DPA. We believe that a more flexible, principle-based approach is needed for this legal ground, allowing for a case-by-case analysis of the interests and safeguards involved.

5. Grounds for processing sensitive data (sections 18-23)

- Given the broad definition of sensitive data, the limited available grounds for processing are particularly troubling. For example, workplaces often process financial data (e.g. HR) or passwords (e.g. IT), limiting the usefulness of processing for employment purposes under section 16.
- We recommend narrowing the definition of sensitive data and introducing reasonable and employment purposes as grounds for processing sensitive data.

6. Data principals' rights (sections 24-28)

- We welcome the list of data principals' rights. Specifically, the right to be forgotten focuses on preventing disclosure, as opposed to an obligation to completely erase data, which is impractical and has a limited privacy benefit.
- The data portability right is expansively drafted and should apply only to raw data provided by the individual, as opposed to insights generated during the provision of the service.
- We recommend inclusion of a deadline for responding to requests of (at least) 30 days and an extension period of 30 days to comply, if justified.

7. Transparency and accountability (sections 29-39)

- Multinationals tend to take global approaches to accountability measures, enabling them to handle data protection at scale with appropriate quality control and governance. As such, we welcome an objective or principle-based approach to such regulatory provisions – as demonstrated in the Privacy by Design section, where however we'd like to see consideration of 'state of the art' and 'cost of implementation' as in the GDPR. The DPA, therefore, should not create mandatory codes of practice in this area that tie companies into a specific approach.
- We recommend that data protection impact assessments (DPIAs) be kept on record internally and provided to the DPA on request, as opposed to automatically submitted. Companies undertake

hundreds of DPIAs and it is not clear what value would be brought by the DPA processing them en masse.

- The DPA should have the power to conduct investigations in the form of data audits, but there should not be a general obligation for fiduciaries to undertake annual audits conducted by registered auditors. This is neither targeted, nor does it reflect that data protection programmes are often managed globally. In fact, audits add a bureaucratic element that does not necessarily increase the level of effective personal data protection for individuals. Accountability and a risk-based approach are better suited for the purposes of data protection laws. Annual audits of all policies and all processing activities by every data fiduciary will not result in meaningful compliance but would certainly considerably increase compliance costs. However, results from independent data audits voluntarily conducted by fiduciaries may, of course, be useful documentation to the DPA during investigations.
- With respect to the requirement to appoint DPOs, we believe this may not be an effective function for all data fiduciaries, irrespective of size or type of processing activities in which they engage. This can be an excessive requirement for certain data fiduciaries that only adds complexity and cost without any significant effect on personal data protection. Similarly to considerations in the GDPR, the Bill should set specific criteria for the obligation of data fiduciaries to appoint DPOs. It should be clarified that for a fiduciary established in India the DPO need not necessarily be located in India – this decision should be left to each organisation based on its internal needs and structure.

8. Security and breach notification (sections 31-32)

- It is important to ensure that only breaches that represent a significant risk are notified to the DPA and individuals to avoid notification fatigue. As such, breaches should be notified to the DPA if there is a real risk of significant material harm to principals; there should be an explicit exemption for data that has been rendered unusable or illegible.
- The mere fact that a system is undergoing maintenance or is offline for other reasons that do not impact privacy does not constitute a breach. The definition of a breach should include permanent loss of data that may be accessible by third parties, but not temporary loss of access to data by data principals.
- Due to the varying nature and complexity of breaches, it would be preferable not to set an explicit deadline for notification but to require notification 'without undue delay' (see Art. 33 GDPR). The timeline for notification should only begin when the responsible team within the fiduciary is aware of the breach and has a sense of its general significance – not when the breach occurs. Breaches may be well disguised (e.g. advanced persistent threats) or originate in third parties, such as the data processor.
- Regardless of the DPA's power to determine whether a breach is notifiable to data principals, fiduciaries should have the right to voluntarily notify data principals prior, or in parallel, to notification of the DPA in order to minimise the impact of a breach.

9. Significant data fiduciaries (section 38)

- The draft bill leaves it to the DPA to determine what entities can be considered 'significant data fiduciaries,' and subsequently what provisions of the law would apply only to them. We would urge greater clarity in the law itself about what entities such classification could apply to; similarly, sub-section 4 introduces the possibility for the DPA to mandate provisions meant for significant data fiduciaries on entities that haven't been classified as such; this provision seems to be in direct contradiction with section 38, which seeks to identify 'significant' entities to which more specific and burdensome obligations should apply.

10. Exemptions (sections 42-48)

- We believe that the exemptions for processing for research purposes should be further specified in the Act rather than left to a future determination by the DPA. This creates an unnecessary bottleneck and we urge greater clarity in the Act itself concerning processing linked to broad societal needs and public interest.

11. Offences (sections 90-96)

- We submit that it is inappropriate for the Act to establish criminal offences. To the extent that violations create criminal as opposed to civil liabilities, they are better described under more specific areas of the penal code (e.g. fraud or cybercrime). Moreover, to the extent that natural persons are acting in the official capacity of the legal person that employs them, they should not be held personally liable. The Bill's imposition of individual liability for 'every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company' is unrealistic given the nature of data governance and data management practices. For example, if the offence consists of the violation of the obligation 'to undertake a data protection impact assessment by a significant data fiduciary under section 33,' the number of persons that may be involved in this violation can be very big, across functions and potentially geographies. This is why liability for such offences lies with the company. The high fines for the company and other non-compliance risk, including reputation damage and loss of business, deter company employees from violating policies that the company needs to establish in order to ensure compliance.

--

For more information please contact:
Alberto Di Felice, DIGITALEUROPE's Senior Policy Manager for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org or +32 2 609 53 10

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total over 35,000 ICT companies in Europe represented by 63 corporate members and 39 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK